PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326920
(43)Date of publication of application : 22.11.2001

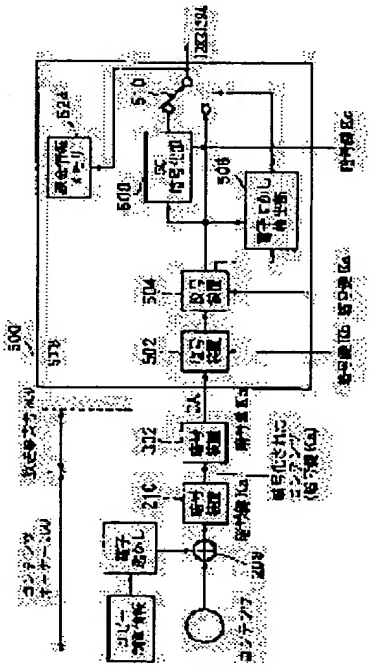
(51)Int.Cl. H04N 7/16
G09C 1/00
G09C 5/00
G11B 20/10
H04H 1/00
H04N 5/44
H04N 7/08
H04N 7/081
H04N 7/167

(21)Application number : 2000-149846
(22)Date of filing : 17.05.2000

(71)Applicant : SONY CORP
(72)Inventor : KORI TERUHIKO
FUJII ASAKO

(54) DATA DISTRIBUTION SYSTEM AND ITS METHOD, DATA RECEIVER, DATA SERVICE DEVICE AND ITS METHOD, AND DATA DELIVERY DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents distribution system with which a right holder can directly control the use of contents data without the aid of a broadcasting entrepreneur while the holder is in the state of capable of connecting a standard I/F and a contents processor.
SOLUTION: A contents owner 200 superposes copy control information by using a digital watermark, and provides the broadcasting entrepreneur 300 with encrypted contents data. The broadcasting entrepreneur 300 distributes by performing encryption for a conditional access. A set top box 500 which received the contents data firstly performs decoding for the conditional access, and secondly performs decoding by using an encryption key distributed by the contents owner 200. Then, the set copy control information is read by extracting digital watermark information, and thus an output from the set top box 500 is controlled.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－326920
（P2001－326920A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04N	7/16		H04N	7/16	Z　5C025
G09C	1/00	660	G09C	1/00	660D　5C063
	5/00			5/00	5C064
G11B	20/10		G11B	20/10	H　5D044
H04H	1/00		H04H	1/00	F　5J104

審査請求　未請求　請求項の数34　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願2000－149846(P2000－149846)

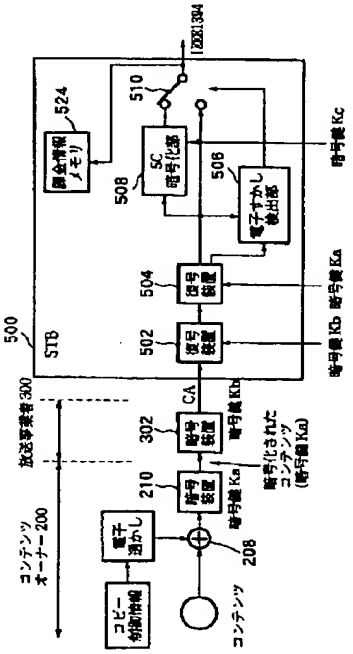
(22)出願日　平成12年５月17日(2000.5.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　郡　照彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　藤井　麻子
アメリカ合衆国　ニュージャージー州　パー　クリッジソニー　ドライブ　ソニー　コーポレーション　オブ　アメリカ内
(74)代理人　100094053
弁理士　佐藤　隆久

最終頁に続く

(54)【発明の名称】　データ配信システムとその方法、データ受信装置、データ提供装置とその方法およびデータ送出装置

(57)【要約】
【課題】標準的なＩ／Ｆおよびコンテンツ処理装置を接続可能な状態でありながら、放送事業者の手を介さずに権利者が直接コンテンツデータの使用を制御することができるコンテンツ配信システムを提供する。
【解決手段】コンテンツオーナー２００は、コピー制御情報を電子透かしにより重畳し、さらに暗号化したコンテンツデータを放送事業者３００に提供する。放送事業者３００はコンディショナルアクセスのための暗号化を行なって配信する。これを受信したセットトップボックス５００では、まずコンディショナルアクセスのための復号を行い、次にコンテンツオーナー２００から配布された暗号鍵を用いて復号を行なう。そして、電子透かし情報を取り出して設定されているコピー制御情報を読み出し、これによりセットトップボックス５００からの出力を制御する。



1

【特許請求の範囲】

【請求項１】所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第１の制御情報を付加し配信対象のデータとして提供するデータ提供手段と、

前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信するデータ送信手段と、

前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御するデータ受信手段とを有するデータ配信システム。

【請求項２】前記データ提供手段は、前記第１の制御情報を電子透かし情報として前記コンテンツデータに重畳し、該重畳されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、

前記データ送信手段は、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記重畳された第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する請求項１に記載のデータ配信システム。

【請求項３】前記データ提供手段は、前記第１の制御情報を電子透かし情報として重畳したコンテンツデータに所定の第１の暗号化を行い、当該暗号化されたデータを前記配信対象のデータとして前記データ送信手段に提供し、

前記データ送信手段は、前記提供された配信対象のデータに前記第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、前記第１の暗号化の復号化を行い前記電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記重畳された第１の制御情報を検出し、該検出された情報に基づいて前記コンテンツデータの出力を制御する請求項２に記載のデータ配信システム。

【請求項４】前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第２の制御情報を付加し、当該第２の制御情報の付加された前記配信対象のデータに前記第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、前記第２の制御情報を検出し、前記復号化された

2

配信対象のデータに前記第１の暗号化の復号化を行い電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記電子透かし情報として重畳された第１の制御情報を検出し、前記検出された第１の制御情報および第２の制御情報に基づいて前記コンテンツデータの出力を制御する請求項３に記載のデータ配信システム。

【請求項５】前記データ提供手段は、前記第１の制御情報を示す制御記述子を前記コンテンツデータに付加し、該制御記述子の付加されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、

前記データ送信手段は、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記付加された第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する請求項１に記載のデータ配信システム。

【請求項６】前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第２の制御情報を付加し、当該第２の制御情報の付加された前記配信対象のデータに前記第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、前記第２情報を検出し、前記復号化された配信対象のデータに前記第１の暗号化の復号化を行い制御記述子が付加されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記制御記述子として付加された第１の制御情報を検出し、前記検出された第１の制御情報および第２の制御情報に基づいて前記コンテンツデータの出力を制御する請求項５に記載のデータ配信システム。

【請求項７】前記データ提供手段は、前記コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第３の制御情報を、当該コンテンツデータに電子透かし情報として重畳し、該第３の制御情報の重畳されたコンテンツデータを前記配信対象のデータとして提供し、

前記データ送信手段は、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された前記第３の制御情報が電子透かし情報として重畳された信号を、要求に応じてアナログ信号出力として出力する請求項１に記載のデータ配信システム。

【請求項８】前記データ受信手段は、前記受信したコンテンツデータの使用状態に基づく、当該コンテンツデータの使用に対する課金に係わる情報を記憶する記憶手段をさらに有する請求項１に記載のデータ配信システム。

【請求項９】所望のコンテンツデータに、当該コンテンツデータの権利者の指示に基づいて当該コンテンツデータの使用状態を制御する第１の制御情報を付加し配信対象のデータとして提供し、

前記提供された配信対象のデータに所定の第２の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、

前記第２の暗号化の復号化を行い、

該復号化された配信対象のデータより前記第１の制御情報を検出し、

該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御するを有するデータ配信方法。

【請求項１０】前記第１の制御情報を電子透かし情報として前記コンテンツデータに重畳し、該重畳されたコンテンツデータを配信対象のデータとして提供し、

前記第１の制御情報の検出は、前記復号化された配信対象のデータより前記電子透かし情報を検出することにより行なう請求項９に記載のデータ配信方法。

【請求項１１】前記第１の制御情報を電子透かし情報として重畳したコンテンツデータに所定の第１の暗号化を行い、当該暗号化されたデータを前記配信対象のデータとして提供し、

前記第２の暗号化の復号化が行なわれたデータに対して、さらに、前記第１の暗号化の復号化を行い、前記電子透かし情報が重畳されたコンテンツデータを生成し、

当該生成されたコンテンツデータより前記重畳された第１の制御情報を検出する請求項１０に記載のデータ配信方法。

【請求項１２】前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第２の制御情報を付加し、

当該第２の制御情報の付加された前記配信対象のデータに前記第２の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、

前記第２の暗号化の復号化を行い、

前記第２の制御情報を検出し、

前記復号化された配信対象のデータに前記第１の暗号化の復号化を行い電子透かし情報が重畳されたコンテンツデータを生成し、

当該生成されたコンテンツデータより前記電子透かし情報として重畳された第１の制御情報を検出し、

前記検出された第１の制御情報および第２の制御情報に基づいて前記コンテンツデータの出力を制御する請求項１１に記載のデータ配信方法。

【請求項１３】前記第１の制御情報の付加は、当該第１の制御情報を示す制御記述子を前記コンテンツデータに付加することにより行い、

前記第１の制御情報の検出は、前記第２の暗号化の復号化が行なわれた配信対象のデータより当該付加された第１の制御情報を検出することにより行なう請求項９に記載のデータ配信方法。

【請求項１４】前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第２の制御情報を付加し、

当該第２の制御情報の付加された前記配信対象のデータに前記第２の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

前記送信された暗号化された配信対象のデータを受信し、

前記第２の暗号化の復号化を行い、

前記第２情報を検出し、

前記復号化された配信対象のデータに前記第１の暗号化の復号化を行い制御記述子が付加されたコンテンツデータを生成し、

当該生成されたコンテンツデータより前記制御記述子として付加された第１の制御情報を検出し、

前記検出された第１の制御情報および第２の制御情報に基づいて前記コンテンツデータの出力を制御する請求項１３に記載のデータ配信方法。

【請求項１５】前記コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第３の制御情報を、当該コンテンツデータの権利者の指示に基づいて、当該コンテンツデータに電子透かし情報として重畳し、該第３の制御情報の重畳されたコンテンツデータを前記配信対象のデータとして提供し、

前記提供された配信対象のデータに所定の第２の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、

前記第２の暗号化の復号化を行い、

少なくともアナログ信号出力が要求された場合には、該復号化された前記第３の制御情報が電子透かし情報として重畳された信号を出力する請求項９に記載のデータ配信方法。

【請求項１６】前記受信したコンテンツデータの使用状態に基づいて、当該コンテンツデータの使用に対する課金を行なう請求項９に記載のデータ配信方法。

【請求項１７】所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第１の制御情報を付加した配信対象のデータに、所定の第２の暗号化を行い送信される信号を受信するデータ受信装置であって、

前記送信された信号を受信する受信手段と、
前記受信した信号に対して前記第２の暗号化の復号化を行う第２の復号化手段と、
前記復号化された配信対象のデータより前記第１の制御情報を検出する第１の制御情報検出手段と、
前記検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する出力制御手段とを有するデータ受信装置。

【請求項１８】前記送信される信号は、前記第１の制御情報が付加されたコンテンツデータに対して、所定の第１の符号化を行い、さらに所定の第２の暗号化を行った信号であり、
前記第２の復号化手段で復号化されたデータに対して前記第１の暗号化の復号化を行なう第１の復号化手段をさらに有し、
前記第１の制御情報検出手段は、前記第１の復号化手段で復号化された結果の前記配信対象のデータより、当該第１の制御情報を検出する請求項１７に記載のデータ受信装置。

【請求項１９】前記第１の復号化手段は、前記コンテンツデータの権利者により配布された所定の鍵データを用いて、前記復号化を行なう請求項１８に記載のデータ受信装置。

【請求項２０】前記第２の復号化手段は、前記信号の送信者により配布された所定の鍵データを用いて、前記復号化を行なう請求項１９に記載のデータ受信装置。

【請求項２１】前記第１の制御情報は電子透かし情報として前記コンテンツデータに重畳されており、
前記第１の制御情報検出手段は、前記復号化された配信対象のデータより前記電子透かし情報として重畳された第１の制御情報を検出する請求項２０に記載のデータ受信装置。

【請求項２２】前記送信される信号は、前記第１の制御情報および当該コンテンツデータの使用状態を制御する第２の制御情報が付加されたコンテンツデータに対して、所定の第１の符号化を行い、さらに所定の第２の暗号化を行った信号であり、
前記復号化された配信対象のデータより前記第２の制御情報を検出する第２の制御情報検出手段と、
前記検出された第１の制御情報および第２の制御情報に基づいて、制御内容を決定する制御内容決定手段とをさらに有し、
前記出力制御手段は、前記決定された制御内容に従って、前記コンテンツデータの出力を制御する請求項１７に記載のデータ受信装置。

【請求項２３】前記第１の制御情報は前記コンテンツデータの権利者により設定された情報であり、
前記第２の制御情報は前記信号の送信者により設定された情報であり、
前記制御内容決定手段は、前記検出された第１の制御情報および第２の制御情報に基づいて、前記コンテンツデータの権利者の設定が、前記信号の送信者の設定よりも優先されるように、前記制御内容を決定する請求項２２に記載のデータ受信装置。

【請求項２４】前記第１の制御情報は制御記述子として前記コンテンツデータに付加されており、
前記第１の制御情報検出手段は、前記復号化された配信対象のデータより前記制御記述子として付加された第１の制御情報を検出する請求項２０に記載のデータ受信装置。

【請求項２５】前記送信される信号は、前記コンテンツデータに、さらに、当該コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第３の制御情報が電子透かし情報として重畳されたデータに基づいた前記信号であり、
前記出力制御手段は、要求応じてアナログ信号により前記コンテンツデータを出力する際には、前記第３の制御情報が電子透かし情報として重畳された信号を出力する請求項１７に記載のデータ受信装置。

【請求項２６】前記受信したコンテンツデータの使用状態に基づく、当該コンテンツデータの使用に対する課金に係わる情報を記憶する記憶手段をさらに有する請求項１７に記載のデータ受信装置。

【請求項２７】所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報を付加する制御情報付加手段と、
前記制御情報が付加されたコンテンツデータを、配信対象のデータとして提供するデータ提供装置。

【請求項２８】前記制御情報の付加されたコンテンツデータを、所定の方式により暗号化する暗号化手段をさらに有し、
前記暗号化されたコンテンツデータを提供する請求項２７に記載のデータ提供装置。

【請求項２９】前記制御情報付加手段は、前記制御情報を、電子透かし情報として前記コンテンツデータに重畳する請求項２８に記載のデータ提供装置。

【請求項３０】前記制御情報付加手段は、前記制御情報を、制御記述子として前記コンテンツデータに付加する請求項２８に記載のデータ提供装置。

【請求項３１】前記コンテンツデータの権利者により指定された、当該コンテンツデータがアナログ信号として出力される際に当該信号の使用状態を制御するアナログ信号制御情報を、電子透かし情報として前記コンテンツデータに重畳するアナログ信号制御情報付加手段をさらに有し、
前記アナログ信号制御情報が重畳されたコンテンツデータを提供する請求項２７に記載のデータ提供装置。

【請求項３２】所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデ

ータの使用状態を制御する制御情報を付加し、
前記制御情報の付加されたコンテンツデータを所定の方式により暗号化し、
該暗号化したコンテンツデータを配信対象のデータとして提供するデータ提供方法。
【請求項３３】前記暗号化されたコンテンツデータを復号化する鍵データは、配信された当該暗号化されたコンテンツデータを受信する受信装置にのみ提供する請求項３２に記載のデータ提供方法。
【請求項３４】所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報が付加され、所定の方式により暗号化された配信対象のデータを、さらに所定の方式により暗号化する暗号化手段と、
前記暗号化した配信対象のデータを任意の伝送路に送出する送出手段とを有するデータ送出装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、所望のコンテンツデータを適切に権利処理を行い配信することのできるデータ配信システムおよびデータ配信方法、配信されるコンテンツデータを受信し適切な権利処理を行なって利用可能に出力するデータ受信装置、コンテンツの権利者がその利用をコントロールできる状態で配信対象のコンテンツデータを提供するデータ提供装置およびデータ提供方法、および、その提供されたデータを送出するデータ送出装置に関する。
【０００２】
【従来の技術】近年、衛星放送やＣＡＴＶなどの種々の形態の放送や、いわゆる放送に限られないたとえばインターネットなどの通信ネットワークを介したデータ配信システムなどの、種々のコンテンツ配信システムが実現されている。そしてそのようなデータ配信システムにおいては、有料で配信されるコンテンツが大きな割合を占めるようになってきている。コンテンツを有料で配信する際の、コンテンツの使用をコントロールする方法としては、コンテンツを暗号化して送出し、受信機器側に暗号を解くためのライセンスを行うことによりコピーコントロールを行なうようにしている場合が多い。ライセンスによって、受信機器側の再生出力自体がコントロールされる。なお、このような観点で言えば、ＤＶＤなどのパッケージメディアを介したコンテンツの配信についても、同様のことが言える。
【０００３】適切なコピーコントロールを行いながら所望のコンテンツを配信する従来のシステムについて、図１０～図１３を参照して説明する。図１０に示すコンテンツ配信システム９１１においては、まず、コンテンツの権利者であるコンテンツオーナー９２０が、暗号化されていないコンテンツを放送事業者９３０に渡す。放送事業者９３０は、暗号鍵Ｋｂを用いてコンディショナルアクセス（ＣＡ）のための暗号化を行い、放送網９４０に送出する。これを受信したセットトップボックス９５０は、予め契約などにより配布されている暗号鍵Ｋｂを用いてコンディショナルアクセスのための暗号化を解く。そして、表示装置９７０との間で伝送を行なうための暗号化を行い、表示装置９７０に対して送出する。なお、セットトップボックス５００と表示装置７００との間の表示装置Ｉ／Ｆ６００は、たとえばＩＥＥＥ１３９４インターフェイスなどが用いられる。その場合、セットトップボックス５００は、復号化したコンテンツデータを５Ｃ－ＤＴＣＰ方式の暗号化を行なう。
【０００４】図１０に示したシステムにおける、コンテンツデータの使用の制御（以後、単にコピー制御と言う場合もある。）の処理について、図１１を参照して詳細に説明する。まず、コピー制御の条件などは、通常コンテンツオーナー９２０が決定する。したがって、コンテンツオーナー９２０は、このコピー制御情報と、コンテンツデータとを放送事業者９３０に提供する。放送事業者９３０は、コンテンツオーナー９００から受け取ったコピー制御情報を制御記述子に変換し、制御記述子付加部９３２においてコンテンツデータに付加する。そして、この制御記述子の付加されたコンテンツデータに対して、放送事業者９３０が、暗号装置９３４において、暗号鍵Ｋｂを用いてコンディショナルアクセスのための暗号化を行い、セットトップボックス９５０に送出する。
【０００５】セットトップボックス９５０においては、復号装置９５２でコンディショナルアクセスのための暗号化が復号化され、制御記述子検出部９５４においてコンテンツデータに付加された制御記述子が検出される。そして、たとえばこの制御記述子に、セットトップボックス９５０から暗号化したコンテンツデータを出力するように記載されていた場合には、制御記述子検出部９５４からの制御信号に基づいて、復号装置９５２からの出力を５Ｃ暗号化部９５６で暗号鍵Ｋｃを用いて暗号化したデータを出力スイッチ９５８において選択し、セットトップボックス９５０より出力する。また、制御記述子に、セットトップボックス９５０から暗号化されていないコンテンツデータを出力してよい旨の記載があった場合には、制御記述子検出部９５４からの制御信号に基づいて、復号装置９５２からの出力を出力スイッチ９５８で選択し、セットトップボックス９５０より出力する。
【０００６】この時に放送事業者９３０で使用される制御記述子の例を図１２に示す。図１２に示すディスクリプタにおいては、（１）の箇所に出力データに対するコピーコントロールタイプとして５Ｃを選択する旨の設定がなされている。また（２）の箇所にコピー制御情報であるＣＧＭＳが記載されている。
【０００７】このようなコンテンツ配信システム９１１においては、暗号化されていないコンテンツ（ソース）

であっても、放送時には暗号鍵Ｋｂのコンディショナルアクセスの暗号化によって守られ、受信後ＣＡを解かれたあとも受信機から出力される際には暗号鍵Ｋｃで暗号化されて伝送されるので、コンテンツのセキュリティは保たれる。また、受信機と表示装置間の接続は放送サービスの形態に係わらず、５Ｃ－ＤＴＣＰ対応のＩＥＥＥ１３９４での標準化が可能であり、受信機と表示装置は標準のものを用いることができる。

【０００８】また、ＸＣＡ(Extended Conditional Access) と呼ばれるコンテンツ配信システムを図１３に示す。このビットストリーム化回路９１２においては、まず、コンテンツオーナー９２０が暗号鍵Ｋａを用いて、コンテンツ自体に暗号をかけて放送事業者９３０に渡す。次に、放送事業者９３０は、暗号鍵Ｋｂを用いて、さらにコンディショナルアクセスのための暗号化を行い送出する。セットトップボックス９５０は、暗号鍵Ｋｂを用いてコンディショナルアクセスを解き、これをそのまま表示装置に送る。この状態でまだコンテンツは暗号化されている。そして、表示装置９７０において、内蔵される復号装置９７２により、暗号鍵Ｋａを用いて暗号化を解き、復号化されたコンテンツを得る。

【０００９】このコンテンツ配信システム９１２においては、最初に暗号化されたコンテンツは、途中の経路では一切暗号が解かれることなく伝送され、表示装置に伝送されて初めて暗号が復号化される仕組みになっている。したがって、伝送経路の装置や放送事業者に不正があるような場合でも、コンテンツの最終到着地である表示装置内でのみ最初の鍵Ｋａによる暗号が復号化されるので安全性が高い。

【００１０】

【発明が解決しようとする課題】しかしながら、図１１を参照して説明した従来のシステムでは、コンテンツオーナーからデータが放送事業者に渡される際には、コンテンツデータも、コピー制御情報も、全く暗号化されていない状態で取り扱われる。その結果、放送事業者が制御記述子を間違えたり、載せるのを誤ったり、あるいは故意に変更したりすると、コンテンツオーナーが意図していた本来のコピー制御、すなわちコンテンツデータの使用の制御が行なえなくなるという問題がある。一方で、図１３を参照して説明した従来のシステムにおいては、安全性が高い反面、表示装置が全て暗号鍵Ｋａによる暗号を復号化できる機能を持つ必要があり、表示装置を標準化、共通化することができないという問題がある。

【００１１】したがって本発明の目的は、受信機より後段の処理装置として標準的な装置を使用しながら、コンテンツオーナーが直接、所望のコピーコントロールを行なうことができるコンテンツ配信システムおよびコンテンツ配信方法を提供することにある。また本発明の他の目的は、そのようなコンテンツ配信システムにおいて用いられ、配信されるコンテンツデータを受信し適切な権利処理を行なって利用可能に出力するデータ受信装置を提供することにある。また本発明の他の目的は、コンテンツの権利者がその利用をコントロールできる状態で配信対象のコンテンツデータを提供するデータ提供装置およびデータ提供方法を提供することにある。さらに本発明の他の目的は、そのように提供されたデータを送出するデータ送出装置を提供することにある。

【００１２】

【課題を解決するための手段】前記課題を解決するために、本発明のデータ配信システムは、所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第１の制御情報を付加し配信対象のデータとして提供するデータ提供手段と、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信するデータ送信手段と、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御するデータ受信手段とを有する。

【００１３】好適には、前記データ提供手段は、前記第１の制御情報を電子透かし情報として前記コンテンツデータに重畳し、該重畳されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記重畳された第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する。

【００１４】また好適には、前記データ提供手段は、前記第１の制御情報を電子透かし情報として重畳したコンテンツデータに所定の第１の暗号化を行い、当該暗号化されたデータを前記配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに前記第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、前記第１の暗号化の復号化を行い前記電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記重畳された第１の制御情報を検出し、該検出された情報に基づいて前記コンテンツデータの出力を制御する。

【００１５】特定的には、前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第２の制御情報を付加し、当該第

２の制御情報の付加された前記配信対象のデータに前記第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、前記第２の制御情報を検出し、前記復号化された配信対象のデータに前記第１の暗号化の復号化を行い電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記電子透かし情報として重畳された第１の制御情報を検出し、前記検出された第１の制御情報および第２の制御情報に基づいて前記コンテンツデータの出力を制御する。

【００１６】また特定的には、前記データ提供手段は、前記第１の制御情報を示す制御記述子を前記コンテンツデータに付加し、該制御記述子の付加されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記付加された第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する。

【００１７】また好適には、前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第２の制御情報を付加し、当該第２の制御情報の付加された前記配信対象のデータに前記第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、前記第２情報を検出し、前記復号化された配信対象のデータに前記第１の暗号化の復号化を行い制御記述子が付加されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記制御記述子として付加された第１の制御情報を検出し、前記検出された第１の制御情報および第２の制御情報に基づいて前記コンテンツデータの出力を制御する。

【００１８】さらに好適には、前記データ提供手段は、前記コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第３の制御情報を、当該コンテンツデータに電子透かし情報として重畳し、該第３の制御情報の重畳されたコンテンツデータを前記配信対象のデータとして提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された前記第３の制御情報が電子透かし情報として重畳された信号を、要求に応じてアナログ信号出力として出力する。好適には、前記データ受信手段は、前記受信したコンテンツデータの使用状態に基づく、当該コンテンツデータの使用に対する課金に係わる情報を記憶する記憶手段をさらに有する。

【００１９】また、本発明に係わるデータ配信方法は、所望のコンテンツデータに、当該コンテンツデータの権利者の指示に基づいて当該コンテンツデータの使用状態を制御する第１の制御情報を付加し配信対象のデータとして提供し、前記提供された配信対象のデータに所定の第２の暗号化を行い、当該暗号化された配信対象のデータを送信し、任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、前記第２の暗号化の復号化を行い、該復号化された配信対象のデータより前記第１の制御情報を検出し、該検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する。

【００２０】また、本発明に係わるデータ受信装置は、所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第１の制御情報を付加した配信対象のデータに、所定の第２の暗号化を行い送信される信号を受信するデータ受信装置であって、前記送信された信号を受信する受信手段と、前記受信した信号に対して前記第２の暗号化の復号化を行う第２の復号化手段と、前記復号化された配信対象のデータより前記第１の制御情報を検出する第１の制御情報検出手段と、前記検出された第１の制御情報に基づいて前記コンテンツデータの出力を制御する出力制御手段とを有する。

【００２１】また、本発明に係わるデータ提供装置は、所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報を付加する制御情報付加手段と、前記制御情報が付加されたコンテンツデータを、配信対象のデータとして提供する。

【００２２】また、本発明に係わるデータ提供方法は、所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報を付加し、前記制御情報の付加されたコンテンツデータを所定の方式により暗号化し、該暗号化したコンテンツデータを配信対象のデータとして提供する。

【００２３】また、本発明に係わるデータ送出装置は、所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報が付加され、所定の方式により暗号化された配信対象のデータを、さらに所定の方式により暗号化する暗号化手段と、前記暗号化した配信対象のデータを任意の伝送路に送出する送出手段とを有する。

【００２４】

【発明の実施の形態】本発明の実施の形態を図１～図９を参照して説明する。

【００２５】全体構成

まず、本実施の形態のコンテンツ配信システムの全体構成について、図１を参照して説明する。図１は、本実施の形態のコンテンツ配信システム１００の全体概略構成を示す図である。コンテンツ配信システム１００は、コンテンツオーナー２００、放送事業者３００、放送網４００、セットトップボックス５００、表示装置Ｉ／Ｆ６００および表示装置７００を有する。

【００２６】まず、各部の構成について説明する。コンテンツオーナー２００は、配信対象のコンテンツの権利者であり、配信対象のコンテンツを所望の暗号鍵Ｋａを用いて暗号化し、暗号化された状態のコンテンツを放送事業者３００に提供する。本実施の形態においては、コンテンツは、たとえばテレビプログラムや映画などの、映像および音声を含むコンテンツとする。なお、ここで言う暗号化とは、コンテンツデータそのもの、あるいはコンテンツオーナー２００が要望する任意の付加データなどを、暗号鍵Ｋａなしでは何ら変更したり読み出したり使用したりすることができない状態にすることを広く指すものとする。したがって、具体的には、実際にコンテンツデータを暗号化する場合、付加データを電子透かしなどの形態で重畳する場合などが含まれる。なお、実際の具体的な処理内容については、後のより具体的な構成の説明の際に説明する。

【００２７】放送事業者３００は、コンテンツオーナー２００より提供された暗号化された状態のコンテンツに、さらに暗号鍵Ｋｂを用いてコンディショナルアクセスのための暗号化を行い、放送網４００を介して配信する。

【００２８】放送網４００は、デジタル地上波放送、デジタル衛星放送、ＣＡＴＶあるいはインターネットなどの通信ネットワークを介した任意のデータ配信システムなどを含む、任意のデータ配信手段であり、放送事業者３００により送出されたコンテンツデータを任意の利用者に配信する。

【００２９】セットトップボックス５００は、たとえば各利用者の家庭などに設けられ、利用者の操作に基づいて、放送網４００を介して放送事業者３００より送出されたデータを受信する受信装置である。セットトップボックス５００は、利用者により選択されたコンテンツデータを受信すると、たとえば予め契約などに基づいて配布される暗号鍵Ｋａを用いて復号化する。そして、予め設定されている暗号鍵Ｋｃを用いてその復号化されたコンテンツデータを再度暗号化し、表示装置Ｉ／Ｆ６００に送出する。本実施の形態においては、セットトップボックス５００と表示装置７００とは、ＩＥＥＥ１３９４をインターフェイスとして接続されており、セットトップボックス５００はＩＥＥＥ１３９４に規定されている５Ｃ暗号化方式によりコンテンツデータを再度暗号化する。

【００３０】表示装置Ｉ／Ｆ６００は、セットトップボックス５００と表示装置７００との間の接続手段であり、前述したように本実施の形態ではＩＥＥＥ１３９４である。

【００３１】表示装置７００は、表示装置Ｉ／Ｆ６００を介してセットトップボックス５００より入力される暗号化されたコンテンツデータを、予め設定されている暗号鍵Ｋｃを用いて復号化し、使用者が視聴可能に表示する。

【００３２】次に、このような構成のコンテンツ配信システム１００の全体の動作の概略について説明する。まず、配信対象のコンテンツは、その権利者であるコンテンツオーナー２００により暗号鍵Ｋａを用いて暗号化された上で放送事業者３００に受け渡され、放送事業者３００によりさらに暗号鍵Ｋｂを用いてコンディショナルアクセスのための暗号化をされ、放送網４００に送出される。

【００３３】放送網４００に送出されたデータは、これを視聴しようとして選択した視聴者（コンテンツの使用者）により、具体的にはその使用者の操作されるセットトップボックス５００により実質的に受信され、内部の復号装置によりまずコンディショナルアクセスのための暗号が復号化される。この時の暗号鍵Ｋａは、使用者が予め放送事業者３００と受信契約を結ぶ際に、たとえばＩＣカードのようなセキュアな記録媒体などの形態で提供される。

【００３４】復号化されたコンテンツデータは、予め設定された暗号鍵Ｋｃを用いてＩＥＥＥ１３９４の５Ｃ方式により再度暗号化され、表示装置７００に送出される。そして、表示装置７００において復号化され、使用者が視聴可能に表示される。なお、視聴者がセットトップボックス５００に対して行なう、受信するコンテンツデータの選択や、セットトップボックス５００から表示装置７００へのコンテンツデータの送出などの操作は、セットトップボックス５００内の課金情報メモリに逐次記憶され、コンテンツ受信に伴う課金に用いられる。

【００３５】このように、コンテンツ配信システム１００においては、コンテンツオーナー２００自体が配信対象のコンテンツに実質的に暗号化を行なっており、またその暗号化は、使用者のセットトップボックス５００まで復号されない構成となっている。したがって、たとえば使用者側におけるコンテンツデータの再生やコピーを制御するコントロール情報を暗号化してコンテンツデータに重畳しておけば、コンテンツオーナー２００自身が使用者側におけるコンテンツデータの使用をコントロールすることができる。すなわち、理由の如何を問わず、放送事業者３００によるコンテンツの使用状態や使用条件などが変更されてしまうことを防ぐことができる。

【００３６】また、コンテンツ配信システム１００においては、コンテンツの使用をそのようなコンテンツオーナー２００のコントロールの範囲内に置きながら、セッ

トトップボックス５００と表示装置７００との間は標準インターフェイスを用いることができる。また、表示装置７００もそのインターフェイスに対応した標準的な装置を用いることができる。

【００３７】具体的適用例

以上、本発明に係わるコンテンツ配信システム１００の全体の構成の概略を説明したが、以下は、より具体的な構成例、具体的な適用形態について、第１の具体例～第５の具体例として説明する。なお、放送網４００、表示装置Ｉ／Ｆ６００および表示装置７００はいずれも標準的なものなので、以下の説明においては、図面上へのその記載および説明を省略する。

【００３８】第１の具体例

コンテンツ配信システム１００の第１の具体的な適用例を、図２を参照して説明する。第１の具体例としては、コンテンツオーナー２００がコンテンツの使用を制御する制御情報を電子透かしの形態でコンテンツデータに重畳して配信し、これにより使用者に受信されたコンテンツデータの使用が制御されるシステムを例示する。図２は、コンテンツ配信システム１００の第１の具体的構成の、コンテンツオーナー２００～セットトップボックス５００までの構成を示す図である。

【００３９】図２に示す第１の具体的構成においては、コンテンツオーナー２００は、電子透かし重畳部２０８を有しており、セットトップボックス５００において有効となるコンテンツの使用を制御するコピー制御情報を、電子透かしの形態でコンテンツデータに重畳する。さらにコンテンツオーナー２００は、暗号装置２１０を有しており、電子透かしの重畳されたコンテンツデータを、暗号鍵Ｋａを用いて暗号化する。そして、この暗号化されたコンテンツデータを放送事業者３００に渡す。

【００４０】放送事業者３００は、暗号装置３０２を有しており、コンテンツオーナー２００から入力されたコンテンツデータに対して、暗号鍵Ｋｂを用いてさらにコンディショナルアクセスのための暗号化を行い送出する。

【００４１】セットトップボックス５００は、２個の復号装置５０２、復号装置５０４、電子透かし検出部５０６、５Ｃ暗号化部５０８、出力スイッチ５１０および課金情報メモリ５２４を有する。復号装置５０２は、放送事業者３００より受信した暗号化された信号を、暗号鍵Ｋｂを用いて復号する。すなわち、コンディショナルアクセスのための暗号化を復号する。復号した信号は、コンテンツオーナー２００により暗号化された信号であり、まだ使用することはできない。

【００４２】復号装置５０４は、復号装置５０２において復号された信号に対して、さらに、暗号鍵Ｋａを用いて復号化し、復号化した信号を電子透かし検出部５０６、５Ｃ暗号化部５０８および出力スイッチ５１０に出力する。復号装置５０４において復号化された信号は、ベースバンドのコンテンツデータにコピー制御情報が電子透かしとして重畳されている信号である。電子透かし検出部５０６は、復号装置５０４において復号された信号より、電子透かしとして重畳されているコピー制御情報を検出し、これに基づいてセットトップボックス５００から出力する信号を制御する信号、具体的には出力スイッチ５１０を制御する信号を生成して、出力スイッチ５１０に印加する。５Ｃ暗号化部５０８は、復号装置５０４において復号された信号を、暗号鍵Ｋｃを用いて５Ｃ方式により暗号化し、出力スイッチ５１０に印加する。

【００４３】出力スイッチ５１０は、電子透かし検出部５０６より印加される制御信号に基づいて、セットトップボックス５００からの出力信号として、復号装置５０４より出力される暗号化されていないコンテンツデータ、あるいは、５Ｃ暗号化部５０８で暗号化されたコンテンツデータのいずれかを選択し、セットトップボックス５００より出力する。課金情報メモリ５２４は、実質的にセットトップボックス５００より出力される信号を検出することにより、あるいは、ＩＥＥＥ１３９４を介して表示装置７００より入力される情報を監視することにより、コンテンツデータの使用に伴う課金に係わる情報を検出し、これを記憶しておく。課金情報メモリ５２４に記憶された情報は、適宜所定の決済機関に送信され、課金処理が行なわれる。

【００４４】このようなセットトップボックス５００においては、復号装置５０２で放送事業者３００により施されたコンディショナルアクセスのための暗号化が復号化され、復号装置５０４でコンテンツオーナー２００自身が施した暗号化が復号化され、その復号化されたコンテンツデータより、電子透かし検出部５０６において、電子透かしとして重畳されているコンテンツオーナー２００により付加されたコピー制御情報が検出される。そして、たとえばこのコピー制御情報に、セットトップボックス５００から暗号化したコンテンツデータを出力するように記載されていた場合には、電子透かし検出部５０６からの制御信号に基づいて、復号装置５０４からの出力を５Ｃ暗号化部５０８で暗号鍵Ｋｃを用いて暗号化したデータを出力スイッチ５１０において選択し、セットトップボックス５００より図示せぬ表示装置に対して出力する。また、コピー制御情報に、セットトップボックス５００から暗号化されていないコンテンツデータを出力してよい旨の記載があった場合には、電子透かし検出部５０６からの制御信号に基づいて、復号装置５０４からの出力を出力スイッチ５１０で選択し、セットトップボックス５００より出力する。

【００４５】このように、第１の具体例においては、コンテンツオーナー２００が電子透かしという形態でコピー制御情報をコンテンツデータに重畳し、さらに暗号化を行なっており、放送事業者３００の手を介することな

く、コンテンツオーナー２００自身が受信側の出力を直接制御することができる。

【００４６】第２の具体例

コンテンツ配信システム１００の第２の具体的な適用例を、図３を参照して説明する。第２の具体例は、第１の具体例におけるコンテンツオーナー２００の暗号装置２１０を無くし、暗号化処理を省略した構成である。またこれに伴って、セットトップボックス５００においても、復号装置５０４が省略された構成となっている。

【００４７】そのような構成においては、コンテンツオーナー２００は、電子透かし重畳部２０８においてコピー制御情報を電子透かしの形態で重畳し、その状態のコンテンツデータをそのまま、すなわち暗号化せずに放送事業者３００に提供する。そして放送事業者３００においては、これを暗号装置３０２でコンディショナルアクセスのための暗号化を行なって送出する。送出さた信号を受信したセットトップボックス５００においては、復号装置５０２でコンディショナルアクセスのための暗号化を復号化することにより、直ちに何ら暗号化されていないコンテンツデータが得られ、これより電子透かし検出部５０６において、電子透かしとして重畳されているコピー制御情報を検出し、これにより出力スイッチ５１０を制御する。５Ｃ暗号化部５０８、出力スイッチ５１０および図示せぬ課金情報メモリなどの動作は、第１の具体例と同じである。

【００４８】このように、第２の具体例においては、コンテンツオーナー２００における暗号装置２１０およびセットトップボックス５００の復号装置５０４が省略されているため、各装置の構成を簡単にすることができる。このような構成においては、コンテンツオーナー２００の暗号装置２１０による暗号化処理がなくなるため、放送事業者３００には暗号化されていない状態のコンテンツデータが渡されることになるが、セットトップボックス５００の出力はあくまでも電子透かし情報により制御されており、また、電子透かしデータが重畳されているため不正利用された場合のトレースが可能であることなどから、不正利用される可能性は低いと言える。このような条件でよければ、構成の簡単なこの第２の具体例が有効である。

【００４９】第３の具体例

コンテンツ配信システム１００の第３の具体的な適用例を、図４および図５を参照して説明する。第３の具体例は、放送事業者３００においてコンテンツオーナー２００が付加するのとは別の独自の制御記述子を付加するようにした構成である。

【００５０】具体的には、コンテンツオーナー２００における処理は、第１の具体例の処理と同じであり、まず、セットトップボックス５００において有効となるコンテンツの使用を制御するコピー制御情報を、電子透かしの形態でコンテンツデータに重畳する。次に、暗号装置２１０において、電子透かしの重畳されたコンテンツデータを、暗号鍵Ｋａを用いて暗号化し、この暗号化されたコンテンツデータを放送事業者３００に渡す。

【００５１】放送事業者３００は、コンテンツオーナー２００から渡された暗号化されたコンテンツデータに対して、制御記述子付加部３０６において、独自の制御記述子を付加し、暗号装置３０２において暗号鍵Ｋｂを用いて暗号化して送出する。

【００５２】これを受信したセットトップボックス５００は、復号装置５０２において放送事業者３００により行なわれたコンディショナルアクセスのための暗号化を暗号鍵Ｋｂを用いて復号する。この復号された信号より、制御記述子検出部５１２において、放送事業者３００が付加した制御記述子が検出され、判定制御装置５１４に出力される。また、復号装置５０２で復号された信号は、さらに復号装置５０４において、暗号鍵Ｋａを用いて復号される。この復号された信号より、電子透かし検出部５０６において、コンテンツオーナー２００が電子透かしの形態で重畳したコピー制御情報が検出され、判定制御装置５１４に出力される。

【００５３】判定制御装置５１４は、電子透かし検出部５０６から入力されるコンテンツオーナー２００により設定されたコピー制御情報、および、制御記述子検出部５１２から入力される放送事業者３００により設定された制御記述子に基づいて、受信したコンテンツデータの使用を制御する判定を行い、その判定に基づいて出力データを制御する。ここで、コピー制御情報および制御記述子には、各々セットトップボックス５００からコンテンツデータを出力する際に、５Ｃ暗号化して伝送するか、暗号化せずに伝送するかの設定が行なわれているものとする。その場合、判定制御装置５１４はたとえば図５に示すようなフローチャートに従って判定を行なう。

【００５４】すなわち、判定を開始すると（ステップＳ１０）、まず、電子透かし検出部５０６から入力されるコピー制御情報を参照して、５Ｃ暗号化の設定が行なわれているか否かを判定する（ステップＳ１１）。そして、５Ｃ暗号化の設定が行なわれていた場合には、出力スイッチ５１０に５Ｃ暗号化部５０８の出力を選択するような制御信号を出力することにより、セットトップボックス５００から５Ｃ暗号化したコンテンツデータを出力させる（ステップＳ１２）。

【００５５】電子透かし検出部５０６から入力されるコピー制御情報に、５Ｃ暗号化の設定が行なわれていなかった場合には（ステップＳ１１）、制御記述子検出部５１２から入力される制御記述子を参照して、５Ｃ暗号化の設定が行なわれているか否かを判定する（ステップＳ１３）。そして、５Ｃ暗号化の設定が行なわれていた場合には、コピー制御情報において設定がなされていた場合と同様に、出力スイッチ５１０に５Ｃ暗号化部５０８の出力を選択するような制御信号を出力し、セットトッ

プボックス５００から５Ｃ暗号化したコンテンツデータを出力させる（ステップＳ１２）。

【００５６】制御記述子検出部５１２から入力される制御記述子にも、５Ｃ暗号化の設定が行なわれていなかった場合には（ステップＳ１３）、判定制御装置５１４は、出力スイッチ５１０に、復号装置５０４からの出力を選択するような制御信号を出力し、セットトップボックス５００から暗号化されていないコンテンツデータを出力させる（ステップＳ１４）。

【００５７】このように、第３の具体例においては、コンテンツオーナー２００および放送事業者３００が、各々独自にコンテンツデータの使用をコントロールする設定を行なうことができる。そして、どちらの設定をどのように優先させて、どのようなコントロールを行なうかは、判定制御装置５１４に設定するアルゴリズムを変えることで任意に設定することができる。そして、たとえば図５に示したようなアルゴリズムを採用することにより、放送事業者３００による設定よりもコンテンツオーナー２００による設定を優先して実行するようにすることができる。

【００５８】第４の具体例

コンテンツ配信システム１００の第４の具体的な適用例を、図６および図７を参照して説明する。第４の具体例は、第３の具体例と同様の構成であるが、コンテンツオーナー２００によるコピーコントロールを、電子透かしをコンテンツデータに重畳することにより行なうのではなく、放送事業者３００と同様に、制御記述子をコンテンツデータに付加することにより行なうようにしたものである。

【００５９】すなわち、コンテンツオーナー２００は、セットトップボックス５００において有効となるコンテンツの使用を制御するコピー制御情報を、制御記述子付加部２１２において、制御記述子（制御記述子１）の形態でコンテンツデータに付加する。そして、その制御記述子の付加されたコンテンツデータに対して、暗号装置２１０において暗号鍵Ｋａを用いて暗号化し、暗号化されたコンテンツデータを放送事業者３００に渡す。放送事業者３００は、コンテンツオーナー２００から渡された暗号化されたコンテンツデータに対して、制御記述子付加部３０６において、独自の制御記述子（制御記述子２）を付加し、暗号装置３０２において暗号鍵Ｋｂを用いて暗号化して送出する。

【００６０】これを受信したセットトップボックス５００は、復号装置５０２において放送事業者３００により行なわれたコンディショナルアクセスのための暗号化を暗号鍵Ｋｂを用いて復号する。この復号された信号より、制御記述子２検出部５１２において、放送事業者３００が付加した制御記述子２を検出し、判定制御装置５１４に出力する。また、復号装置５０２で復号された信号は、さらに復号装置５０４において、暗号鍵Ｋａを用いて復号される。そしてこの復号された信号より、制御記述子１検出部５１６において、コンテンツオーナー２００が付加した制御記述子１を検出し、判定制御装置５１４に出力する。

【００６１】判定制御装置５１４は、制御記述子１検出部５１６から入力されるコンテンツオーナー２００により設定された制御記述子１、および、制御記述子２検出部５１２から入力される放送事業者３００により設定された制御記述子２に基づいて、受信したコンテンツデータの使用を制御する判定を行い、その判定に基づいて出力データを制御する。ここで、制御記述子１および制御記述子２には、各々セットトップボックス５００からコンテンツデータを出力する際に、５Ｃ暗号化して伝送するか、暗号化せずに伝送するかの設定が行なわれているものとする。その場合、判定制御装置５１４はたとえば図７に示すようなフローチャートに従って判定を行なう。

【００６２】すなわち、判定を開始すると（ステップＳ２０）、まず、制御記述子１検出部５１６から入力される制御記述子１を参照して、５Ｃ暗号化の設定が行なわれているか否かを判定する（ステップＳ２１）。そして、５Ｃ暗号化の設定が行なわれていた場合には、出力スイッチ５１０に５Ｃ暗号化部５０８の出力を選択するような制御信号を出力することにより、セットトップボックス５００から５Ｃ暗号化したコンテンツデータを出力させる（ステップＳ２２）。

【００６３】制御記述子１検出部５１６から入力される制御記述子１に、５Ｃ暗号化の設定が行なわれていなかった場合には（ステップＳ２１）、制御記述子２検出部５１２から入力される制御記述子２を参照して、５Ｃ暗号化の設定が行なわれているか否かを判定する（ステップＳ２３）。そして、５Ｃ暗号化の設定が行なわれていた場合には、制御記述子１において設定がなされていた場合と同様に、出力スイッチ５１０に５Ｃ暗号化部５０８の出力を選択するような制御信号を出力し、セットトップボックス５００から５Ｃ暗号化したコンテンツデータを出力させる（ステップＳ２２）。

【００６４】制御記述子２検出部５１２から入力される制御記述子２にも、５Ｃ暗号化の設定が行なわれていなかった場合には（ステップＳ２３）、判定制御装置５１４は、出力スイッチ５１０に、復号装置５０４からの出力を選択するような制御信号を出力し、セットトップボックス５００から暗号化されていないコンテンツデータを出力させる（ステップＳ２４）。

【００６５】このように、第４の具体例においては、コンテンツオーナー２００および放送事業者３００は、ともに制御記述子を付加するという形態で、各々独自にコンテンツデータの使用をコントロールする設定を行なうことができる。そして、どちらの設定をどのように優先させて、どのようなコントロールを行なうかは、判定制

御装置５１４に設定するアルゴリズムを変えることで任意に設定することができる。そして、たとえば図７に示したようなアルゴリズムを採用することにより、放送事業者３００による設定よりもコンテンツオーナー２００による設定を優先して実行するようにすることができる。

【００６６】第５の具体例

コンテンツ配信システム１００の第５の具体的な適用例を、図８を参照して説明する。第５の具体例は、セットトップボックス５００からのアナログの出力に対しても、適切にコピーコントロールが行なえるようにしたものである。

【００６７】この場合、まずコンテンツオーナー２００は、設定したいコピー制御情報を、電子透かし重畳部２０８において、電子透かしの形態でコンテンツデータに重畳する。この電子透かし情報は、セットトップボックス５００からのアナログ出力のコピープロテクションに用いられる。そしてコンテンツオーナー２００は、その電子透かし情報の重畳されたコンテンツデータに対して、暗号装置２１０において暗号鍵Ｋａを用いて暗号化する。この、暗号化されたコンテンツデータと、先のコピー制御情報の両方を、コンテンツオーナー２００は放送事業者３００に渡す。

【００６８】放送事業者３００は、コンテンツオーナー２００から渡されたコピー制御情報を制御記述子に変換した後、これを、制御記述子付加部３０６において、コンテンツオーナー２００から渡された暗号化されたコンテンツデータに付加し、暗号装置３０２において暗号鍵Ｋｂを用いて暗号化して送出する。

【００６９】これを受信したセットトップボックス５００は、復号装置５０２において放送事業者３００により行なわれたコンディショナルアクセスのための暗号化を暗号鍵Ｋｂを用いて復号する。この復号された信号より、制御記述子検出部５１２において、コンテンツオーナー２００からの指示により放送事業者３００が付加した制御記述子を検出し、出力スイッチ５１０を制御する制御信号を生成して出力スイッチ５１０に印加する。また、復号装置５０２で復号された信号は、さらに復号装置５０４において、暗号鍵Ｋａを用いて復号される。この復号化された信号は、５Ｃ暗号化部５０８において５Ｃ暗号化されて、あるいは、直接、出力スイッチ５１０に印加され、出力スイッチ５１０でいずれかが選択してデジタル出力として出力される。一方、復号装置５０２で復号された信号は、アナログ信号エンコーダ５１８に入力されて、ここでアナログ信号に変換されて、セットトップボックス５００より出力される。

【００７０】このように、第５の具体例においては、特に、セットトップボックス５００より、電子透かしにより著作権保護情報が重畳された適切に権利処理されたアナログ信号を出力することができる。したがって、アナログ信号出力を必要とする場合には好適である。

【００７１】なお、図８に示した構成においては、コンテンツオーナー２００が要求するコピー制御情報を、放送事業者３００が制御記述子に変換してコンテンツデータに付加している。放送事業者３００が十分信頼のおける機関であれば、このような構成として何ら問題はない。しかし、何らかの理由でコンテンツオーナー２００が自ら設定を行う場合には、第３の具体例の場合と同様に、制御記述子の設定もコンテンツオーナー２００が行なうようにしてよい。

【００７２】第６の具体例

コンテンツ配信システム１００の第６の具体的な適用例を、図９を参照して説明する。第６の具体例は、セットトップボックス５００からのデジタル出力を、モニタ接続用のＤＶＩ(Digital Visual Interface)およびその著作権保護された出力（ＤＶＩ－ＣＰ）のいずれかとし、また、アナログ出力をＯＮ／ＯＦＦできるようにしたものである。

【００７３】この場合、コンテンツオーナー２００は、電子透かし重畳部２０８において、設定したいコピー制御情報を電子透かしの形態でコンテンツデータに重畳し、暗号装置２１０において、その電子透かし情報の重畳されたコンテンツデータを暗号鍵Ｋａを用いて暗号化し、暗号化されたコンテンツデータを、放送事業者３００に渡す。

【００７４】放送事業者３００は、制御記述子付加部３０６において、独自の制御記述子をコンテンツオーナー２００から渡された暗号化されたコンテンツデータに付加した後、暗号装置３０２において暗号鍵Ｋｂを用いてコンディショナルアクセスのための暗号化を行い、送出する。

【００７５】これを受信したセットトップボックス５００は、復号装置５０２において、放送事業者３００により行なわれたコンディショナルアクセスのための暗号化を暗号鍵Ｋｂを用いて復号し、制御記述子検出部５１２において、この復号された信号より放送事業者３００が付加した制御記述子を検出し、判定制御装置５１４に出力する。また、復号装置５０２で復号された信号は、さらに復号装置５０４において、暗号鍵Ｋａを用いて復号され、この復号された信号より、電子透かし検出部５０６において、コンテンツオーナー２００が電子透かしの形態で重畳したコピー制御情報が検出され、判定制御装置５１４に出力される。

【００７６】判定制御装置５１４は、電子透かし検出部５０６から入力されるコンテンツオーナー２００により設定されたコピー制御情報、および、制御記述子検出部５１２から入力される放送事業者３００により設定された制御記述子に基づいて、受信したコンテンツデータの使用を制御する判定を行い、その判定に基づいて出力データを制御する。具体的には、判定制御装置５１４は、

セットトップボックス５００からのデジタル出力として、ベースバンドデータの出力を行なうか、ＤＶＩ－ＣＰにより暗号化されたデータを出力するかの判定、および、アナログ出力を行なうか否かの判定を行ない、各々その判定結果に基づく制御信号を、出力スイッチ５１０およびアナログ出力スイッチ５２２に出力する。

【００７７】また、復号装置５０４において復号化された信号は、暗号化部５２０においてＤＶＩ－ＣＰに暗号化されて、あるいは、直接、出力スイッチ５１０に印加され、出力スイッチ５１０でいずれかが選択してデジタル出力として出力される。一方、復号装置５０４で復号された信号は、アナログ信号エンコーダ５１８に入力されて、ここでアナログ信号に変換されて、アナログ出力スイッチ５２２に印加され、判定制御装置５１４の制御に基づいてアナログ出力スイッチ５２２において選択され、アナログ出力として出力される。

【００７８】このように、第６の具体例においては、セットトップボックス５００から、ＤＶＩにより、ＲＧＢベースバンド信号あるいは符号化された信号として、デジタル映像信号を出力することができる。また、電子透かしにより著作権保護情報が重畳された適切に権利処理されたアナログ信号を、選択的に出力することができる。

【００７９】変形例

なお、本発明は本実施の形態に限られるものではなく、任意好適な種々の改変が可能である。たとえば、コンテンツ配信システム１００においてセットトップボックス５００に接続されて利用される装置は、映像信号を表示する表示装置としたが、これに限られるものではなく、任意の画像処理装置を接続するようにしてよい。たとえば、出力されるデータを記録する記録装置を接続してもよいし、出力されるデータを伝送する伝送装置などを接続してもよい。また、セットトップボックス５００の出力Ｉ／Ｆも、前述した実施の形態中で示したＩＥＥＥ１３９４およびＤＶＩに限られるものではなく、任意のＩ／Ｆを用いてよい。

【００８０】また、放送事業者３００とセットトップボックス５００との間でデータを伝送する手段は、放送手段に限られるものではなく、任意の情報伝送手段を適用してよい。また、いわゆる放送に限られるものではなく、セットトップボックス５００からの要求に応じて所望のコンテンツデータを要求のあったセットトップボックス５００に送信するような伝送手段であってもよい。

【００８１】また、本実施の形態においては、配信されるコンテンツは映像信号およびオーディオ信号を含むビデオ信号としたが、これに限られるものではなく、任意のコンテンツデータの配信に適用してよい。たとえば、オーディオデータ、静止画像データ、ゲームソフトプログラム、任意のプログラムソフトなどの配信システムとして使用してよい。

【００８２】

【発明の効果】このように本発明によれば、受信機より後段の処理装置として標準的な装置を使用しながら、コンテンツオーナーが直接、所望のコピーコントロールを行なうことができるコンテンツ配信システムおよびコンテンツ配信方法を提供することができる。また、そのようなコンテンツ配信システムにおいて用いられ、配信されるコンテンツデータを受信し適切な権利処理を行なって利用可能に出力するデータ受信装置を提供することができる。また、コンテンツの権利者がその利用をコントロールできる状態で配信対象のコンテンツデータを提供するデータ提供装置およびデータ提供方法を提供することができる。さらに、そのように提供されたデータを送出するデータ送出装置を提供することができる。

【図面の簡単な説明】

【図１】図１は、本発明の一実施の形態のコンテンツ配信システムの全体概略構成を示す図である。

【図２】図２は、図１に示したコンテンツ配信システムの第１の具体例の主要部の構成を示す図である。

【図３】図３は、図１に示したコンテンツ配信システムの第２の具体例の主要部の構成を示す図である。

【図４】図４は、図１に示したコンテンツ配信システムの第３の具体例の主要部の構成を示す図である。

【図５】図５は、図４に示したセットトップボックスの判定制御装置における判定処理を説明するためのフローチャートである。

【図６】図６は、図１に示したコンテンツ配信システムの第４の具体例の主要部の構成を示す図である。

【図７】図７は、図６に示したセットトップボックスの判定制御装置における判定処理を説明するためのフローチャートである。

【図８】図８は、図１に示したコンテンツ配信システムの第５の具体例の主要部の構成を示す図である。

【図９】図９は、図１に示したコンテンツ配信システムの第６の具体例の主要部の構成を示す図である。

【図１０】図１０は、従来のコンテンツ配信システムの全体概略構成を示す図である。

【図１１】図１１は、図１０に示したコンテンツ配信システムの第１の具体例の主要部の構成を示す図である。

【図１２】図１２は、図１１に示した放送事業者で付加する制御記述子の具体例を示す図である。

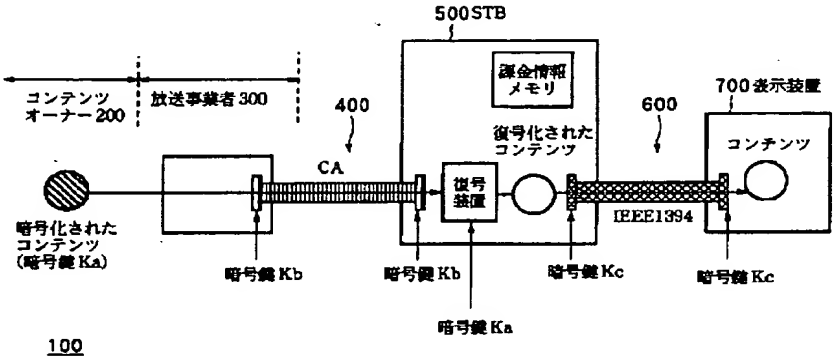
【図１３】図１３は、図１０に示したコンテンツ配信システムの第２の具体例の主要部の構成を示す図である。

【符号の説明】

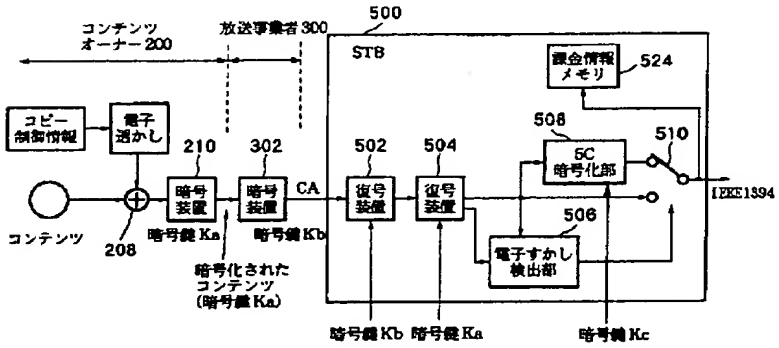
１００…コンテンツ配信システム、２００…コンテンツオーナー、２０８…電子透かし重畳部、２１０…暗号装置、２１２…制御記述子付加部、３００…放送事業者、３０２…暗号装置、３０６…制御記述子付加部、４００…放送網、５００…セットトップボックス、５０２…復号装置、５０４…復号装置、５０６…電子透かし検出

部、５０８…５C暗号化部、５１０…出力スイッチ、５１２…制御記述子検出部、５１４…判定制御装置、５１６…制御記述子１検出部、５１８…アナログ信号エンコーダ、５２０…暗号化部、５２２…アナログ出力スイッチ、５２４…課金情報メモリ、６００…表示装置Ｉ／Ｆ、７００…表示装置、９１１、９１２…コンテンツ配＊信システム、９２０…コンテンツオーナー、９３０…放送事業者、９３２…制御記述子付加部、９３４…暗号装置、９４０…放送網、９５０…セットトップボックス、９５２…復号装置、９５４…制御記述子検出部、９５６…５C暗号化部、９５８…出力スイッチ、９７０…表示装置

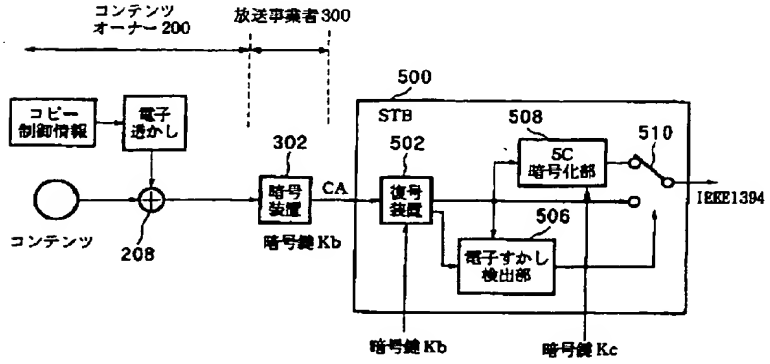
【図１】



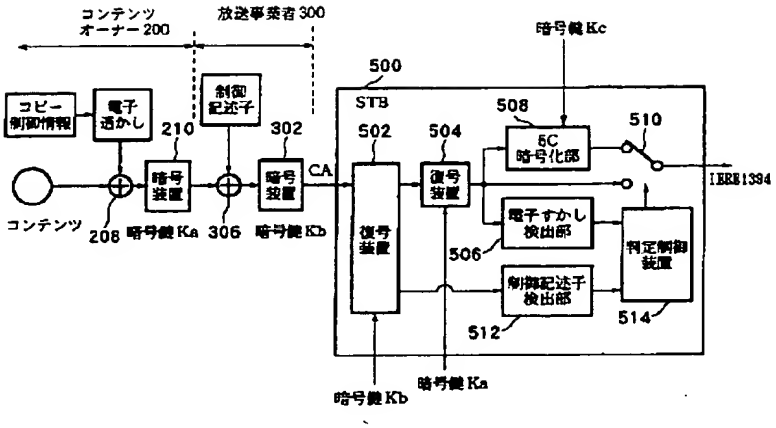
【図２】



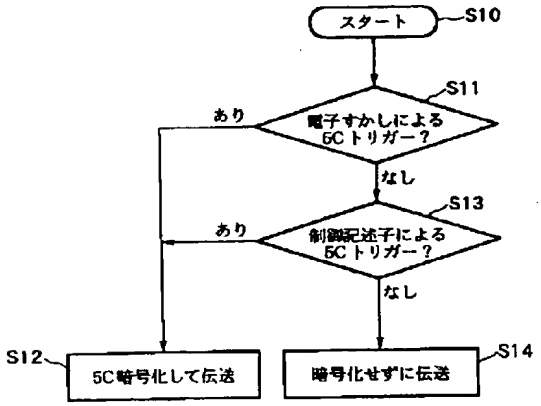
【図３】



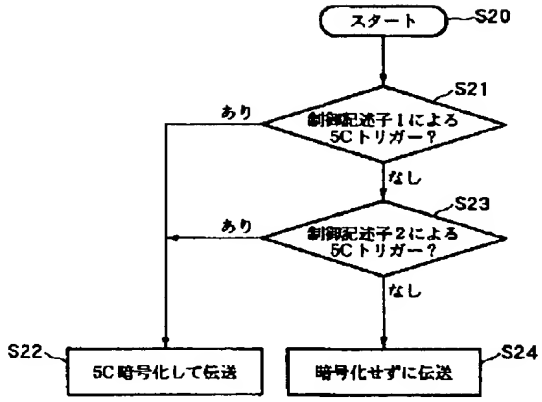
【図４】


コンテンツ
オーナー200
放送事業者300
コピー
制御情報
電子
透かし
制御
記述子
210
302
暗号
装置
暗号
装置
CA
コンテンツ
208
暗号鍵Ka
306
暗号鍵Kb
500
STB
502
504
508
5C
暗号化部
510
IEEE1394
復号
装置
復号
装置
電子すかし
検出部
506
制御記述子
検出部
判定制御
装置
512
514
暗号鍵Kc
暗号鍵Kb
暗号鍵Ka

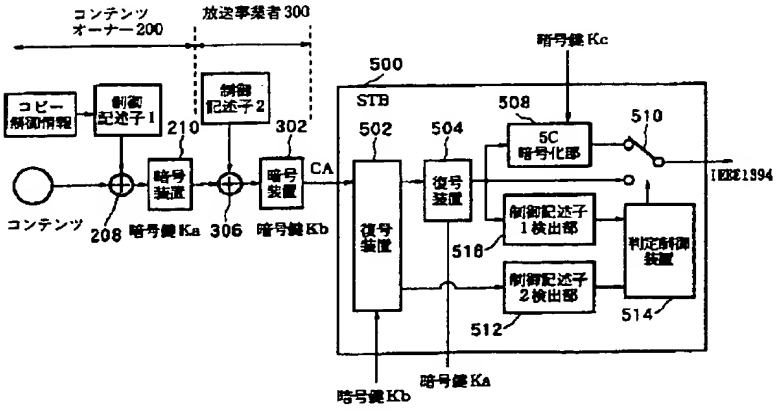
【図５】


スタート
S10
S11
電子すかしによる
5Cトリガー？
あり
なし
S13
制御記述子による
5Cトリガー？
あり
なし
S12
5C暗号化して伝送
暗号化せずに伝送
S14

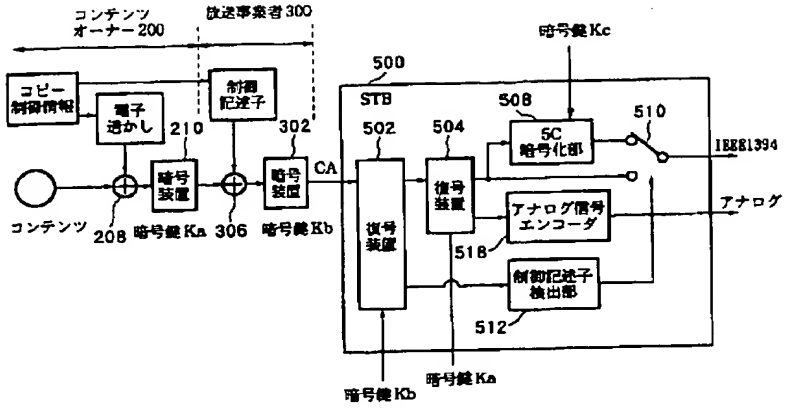
【図７】


スタート
S20
S21
制御記述子１による
5Cトリガー？
あり
なし
S23
制御記述子２による
5Cトリガー？
あり
なし
S22
5C暗号化して伝送
暗号化せずに伝送
S24

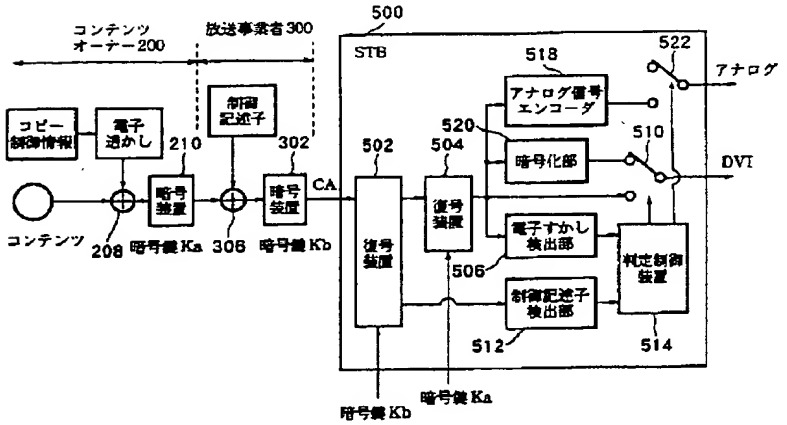
【図６】


コンテンツ
オーナー200
放送事業者300
コピー
制御情報
制御
記述子１
制御
記述子２
210
302
暗号
装置
暗号
装置
CA
コンテンツ
208
暗号鍵Ka
306
暗号鍵Kb
500
STB
502
504
508
5C
暗号化部
510
IEEE1394
復号
装置
復号
装置
制御記述子
１検出部
518
制御記述子
２検出部
判定制御
装置
512
514
暗号鍵Kc
暗号鍵Kb
暗号鍵Ka

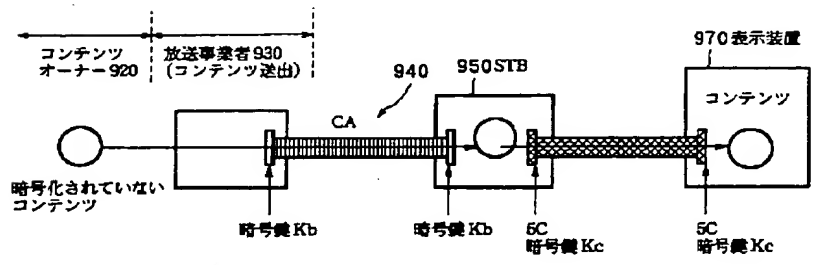
【図８】


コンテンツ
オーナー200
放送事業者300
コピー
制御情報
電子
透かし
制御
記述子
210
302
暗号
装置
暗号
装置
CA
コンテンツ
208
暗号鍵Ka
306
暗号鍵Kb
500
STB
502
504
508
5C
暗号化部
510
IEEE1394
復号
装置
復号
装置
アナログ信号
エンコーダ
アナログ
518
制御記述子
検出部
512
暗号鍵Kc
暗号鍵Kb
暗号鍵Ka

【図９】

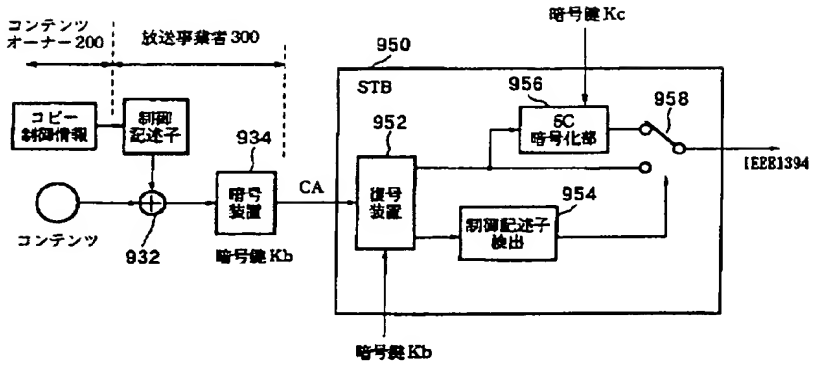

コンテンツ
オーナー200
放送事業者300
500
STB
518
522
アナログ
アナログ信号
エンコーダ
コピー
制御情報
電子
透かし
制御
記述子
210
302
520
510
暗号化部
DVI
502
504
暗号
装置
暗号
装置
CA
復号
装置
復号
装置
電子すかし
検出部
506
判定制御
装置
制御記述子
検出部
512
514
コンテンツ
208
暗号鍵Ka
306
暗号鍵Kb
暗号鍵Kb
暗号鍵Ka

【図１０】


コンテンツ
オーナー920
放送事業者930
(コンテンツ送出)
940
950STB
970表示装置
コンテンツ
CA
暗号化されていない
コンテンツ
暗号鍵Kb
暗号鍵Kb
5C
暗号鍵Kc
5C
暗号鍵Kc

911

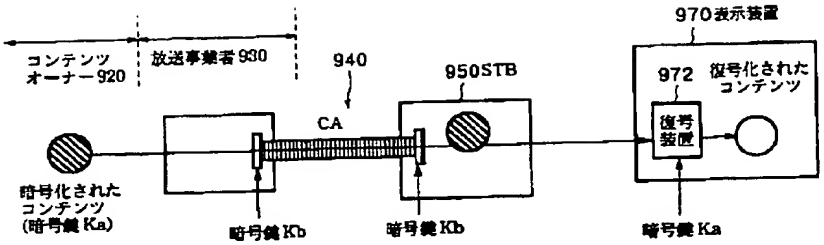
【図１１】



【図１２】

```
digital_copy_control_descriptor ( ) {
    descriptor_tag
    descriptor_length
    digital_recording_control_data
    maximum_bit_rate_flag
    component_control_flag
    copy_control_type
    if(copy_control_type==01))    ←― (1) 5Cを選択
            APS_control_data
    }
    else {
            reserved_future_use
    }
    if(maximum_bit_rate_flag==1){
        maximum_bit_rate
    }
    if(component_control_flag==){
        component_control_length
        for(j=0;j<N;j++) {
            component_tag
            digital_recording_control_data ←― (2) CGMSを伝送
            maximum_bitrate_flag
            reserved_future_use
            copy_control_type
            if(copy_control_type==01){
                    APS_control_data
            }
            else {
                    reserved_future_use
            }
            if(maximum_bitrate_flag==1){
                maximum_bitrate
            }
        }
    }
}
```

【図１３】



912

フロントページの続き

(51) Int. Cl.'		識別記号	F I		テーマコード' (参考)
Ｈ０４Ｎ	5/44		Ｈ０４Ｎ	5/44	A
	7/08			7/08	Z
	7/081			7/167	Z
	7/167				

Ｆターム(参考)　5C025 BA25 DA01 DA04 DA05
5C063 AA01 AB03 AB05 AB09 AC01
CA12 CA23 CA36 DA07 DA13
5C064 CA14 CB01
5D044 BC03 CC04 DE42 DE49 DE50
GK17 HL08 HL11
5J104 AA01 AA14 BA03 PA04 PA06